Schrems II: The Right to Privacy and the New Illiberalism

Francesca Bignami 2020-07-29T13:05:41

On its face, *Schrems II* is a sequel. Decided on July 16, 2020, the Court of Justice of the EU (CJEU) found that the EU-US data protection agreement ("Privacy Shield") that had served as one of the bases for Facebook's transfer of personal data to the US was invalid. Because Privacy Shield could not guarantee an adequate level of protection for EU personal data in the event of access by US intelligence agencies, the CJEU found that it was in violation of the right to data protection. This judgment was handed down five years after *Schrems I*, where the CJEU had ruled that Privacy Shield's predecessor agreement was invalid, in litigation involving the same parties, the same, Irish, Data Protection Authority (DPA), and the same US intelligence programs.

But for all the similarities, it is critical to appreciate that the judgment in *Schrems II* speaks to a radically changed political world. Since 2015, when *Schrems I* was decided, a lot has happed. First, as has been extensively documented in the press and official reports, Russia, Cambridge Analytica, and other bad actors have exploited the privacy vulnerabilities of US-based Facebook to interfere with elections and democratic societies. Second, in November 2016, Trump was elected US President and since then he and his administration have undermined fundamental principles of US liberal democracy. Third, in June 2016, the UK voted to leave the EU, and on January 31, 2020, it did, taking with it its powerful security and intelligence apparatus (subject to a transitional period that expires on December 31, 2020). Fourth, all the while, EU Member States have enacted expansive surveillance laws, some in response to terrorist attacks like the Paris one in November 2015, others as part of a larger pattern of democratic backsliding.

The rest of this post unpacks the implications of *Schrems II* for this new, unstable, and in many instances, illiberal political landscape. A number of excellent posts on this blog (here, here and here) have already examined the impact of *Schrems II* on the corporate actors that transfer EU data globally. My focus here is on how *Schrems II* and the CJEU's evolving jurisprudence on the right to privacy can be read as targeting the political developments of recent years.

Interference with democracy through Facebook (and other global communications actors)

First, interference with democracy through Facebook: One of the important lessons of the past five years has been that privacy breaches, wherever they occur, make democracies vulnerable, wherever they are. The first part of *Schrems II* details how, under EU law, EU privacy officials should address this problem. There the CJEU

discusses the EU's interlocking system of standard contractual clauses (SCCs) and third-country adequacy decisions for protecting the privacy of EU personal data when it is transferred abroad by corporate actors. A SCC is what Facebook relied on for making data transfers to the US but the adequacy decision (based on Privacy Shield) was also necessary, to guarantee respect for privacy if Facebook data ended up in the hands of the US government.

What is striking is the CJEU's emphasis on the duties and powers of DPAs to enforce EU privacy standards when data is sent abroad. This has always been a secondary area of DPA activity, in my view because of the discrepancies between DPA resources and the corporate actors and the foreign jurisdictions that they are supposed to be monitoring. How exactly is the relatively small Irish DPA supposed to monitor the third-country transfers of the disproportionate number of digital multinationals that have established their EU internal market presence via Ireland? As a result, historically, most of the action on third-country transfers has been at the EU level, in the form of European Commission third-country adequacy decisions, standard contractual clauses, and binding corporate rules.

In *Schrems II*, however, the CJEU came down in favor of more DPA enforcement in the context of third-country transfers. In its detailed description of the enforcement system, the DPAs are the essential backstop for contractually-based transfers to third countries: if they find that the terms of standard contractual clauses are not being complied with in third countries, they must either suspend or prohibit the transfer (paras. 145-148). Even in the case of third-country transfers based on adequacy decisions, DPAs play an essential role: as the Irish DPA did in *Schrems II* with respect to the Privacy Shield decision, DPAs are obliged to refer any doubts as to whether a country has "adequate" privacy to their national courts, which in turn are to refer the issue to the CJEU (paras. 119, 120). Ultimately, the upshot of more DPA enforcement will be the need for more data localization by commercial actors—something that the CJEU has already indicated for law enforcement actors in its *Tele2* judgment.

The Trump administration

Second, the Trump administration: The first part of the *Schrems II* judgment and its emphasis on enforcement applies not just to data transfers to the US but to all foreign jurisdictions. As many *Schrems II* commentators have correctly noted, ensuring adequacy is far more difficult, and unlikely, in the case of transfers to authoritarian regimes like China. But the second part of *Schrems II* concerns specifically the (in)adequacy of US privacy guarantees for EU personal data in intelligence surveillance. In assessing (in)adequacy, the CJEU's analysis was strictly limited to the US law on the books. However, it certainly didn't help that the Trump administration has relentlessly politicized and circumvented the executive branch, including the intelligence and foreign policy establishment, which in the Privacy Shield bore significant responsibility for protecting EU privacy.

As is well known, there is a legal vacuum in US constitutional law for the privacy of non-US persons. (In statutory law, a "US person" is defined as either a citizen or

a permanent resident, and a “non-US person” as everyone else; the constitutional law case on point speaks of foreign citizens and residents “with no voluntary attachment” to the US.) Since 9/11 , this constitutional vacuum has been used first by the President (under Article II) and then by Congress (with the enactment of Section 702 of the FISA Amendments Act) to expand the surveillance powers of the intelligence community and, to a lesser extent, law enforcement. In the long fall out from the Snowden revelations, US diplomacy has been geared at assuring the EU that the surveillance of non-US persons in the *institutional practice* of the executive branch is far less expansive and much more privacy protective than it might seem from the *letter of the law*. This was the gist of President Obama’s PPD-28 and the Office of the Director of National Intelligence, Department of Justice, and State Department annexes to the Privacy Shield.

Even pre-Trump, the executive branch assurances given in PPD-28 and the Privacy Shield would likely not have convinced the CJEU. In *Schrems II*, the absence of recourse to an independent court was the major flaw with the US system that was singled out by the CJEU. Effective judicial redress has always been essential to the CJEU’s data protection jurisprudence and the fact of the matter is that it doesn’t exist in intelligence surveillance, especially for non-US persons. However, Trump’s election and the breakdown of a variety of institutional norms, sealed Privacy Shield’s fate.

In the Privacy Shield, an ombudsman within the State Department was supposed to serve as the executive branch’s institutional alternative to courts. To quote from the State Department’s website:

> The Under Secretary [i.e. the Privacy Shield Ombusdman] reports directly to the Secretary of State and is independent from the Intelligence Community. To carry out the Ombudsperson duties, the Under Secretary works closely with other United States Government officials, *including independent oversight bodies such as inspectors general,* as appropriate, to ensure that completed requests are processed and resolved in accordance with applicable laws and policies [emphasis added].

But without any apparent legal or even significant political fallout, Trump dismissed first the Inspector General for the Intelligence Community in April 2020 and then the Inspector General for the State Department in May 2020. Under such conditions, where dismissal appears to be entirely at will, it is difficult to believe the claim of independence.

In short, the credibility of the internal, executive branch safeguards detailed in the Privacy Shield has suffered during the Trump administration. The CJEU’s repeated insistence in *Schrems II* on independent courts as the essential guarantors of privacy can be seen, at least in part, as a response to this experience.

Brexit

Third, Brexit: Once the Brexit transitional period expires on December 31, 2020, the UK will be, legally speaking, a third country. In *Schrems II*, the CJEU made it clear that, as a third country, all aspects of the UK's privacy regime, including national security, will fall under the scope of the General Data Protection Regulation (GDPR), and will be subject to the requirement of adequacy (paras. 87-88). Moreover, the CJEU said that the analysis of third-country adequacy proceeds entirely based on the GDPR, read in light of the EU Charter of Fundamental Rights (para. 101)—not the European Convention of Human Rights, which is believed by many to be less demanding on the privacy issue. This is particularly significant for the UK since its security and intelligence agencies conduct extensive bulk interception, collection, and "equipment interference," i.e. hacking.

Beyond the UK's own surveillance capacity, it is known to collaborate extensively with foreign governments, including the US, as part of the Five Eyes Agreement. For law enforcement purposes, now there is also the UK-US CLOUD Act Agreement for police access to stored communications, as well as for real-time wiretaps of wire and electronic communications; this agreement specifically contemplates US access to the communications of third-country nationals handled by UK providers, e.g. EU persons. As the prospect of a "hard" Brexit has become a reality, the UK government has pivoted even closer to the US, with implications for more US-UK data sharing and privacy rights—and for the adequacy of UK law from the perspective of EU personal data.

A good preview of what the Brexit future might look like is *Elgizouli v. Secretary of State for the Home Department*. That case involved a UK MLAT transfer of criminal evidence to the US, without the standard assurances from the US government of (not) seeking the death penalty. The UK Supreme Court found that the UK government's transfer was unlawful because the government had failed to comply with the UK Data Protection Act 2018, which poses strict limitations on third-country transfers for law enforcement purposes. In the future however, with the many anticipated changes that will be made to statutory law, the UK courts will not be able to exercise the same judicial review powers. *Schrems II* serves as a useful affirmation and reminder that EU law, EU DPAs, and the CJEU will step in when EU personal data is at stake.

Expansive surveillance laws in the EU Member States

Fourth and last, crisis-fueled, expansive surveillance legislation in many Member States: For various reasons, European statutory law has typically not relied on the categorical distinction between foreigners and citizens/permanent residents that is so important for US privacy law. In a set of recently decided fundamental rights cases (for the European Court of Human Rights, see the German Constitutional Court's discussion at para. 271), this is becoming a matter of constitutional law too —foreigners without any physical connection to the territory of the surveilling nation

nonetheless have rights if they are subject to the surveillance of that nation. What is striking, however, are the surveillance powers that are emerging in some places with respect to all persons, including resident nationals. A Swedish intelligence law that was litigated, and found to be lawful by the European Court of Human Rights, provides for intelligence interception, based on "tasking directives," of all "cable-based cross-border communications"—surveillance powers that do not seem far off from the National Security Agency's Section 702 programs, but without the safeguards that exist there for US persons. In the CJEU, there is currently a pending UK case that involves intelligence orders for bulk communications data—something that is simply a more tailored version of the National Security Agency's original Section 215 program. There is also a pending French case, where among the intelligence tools at issue is real-time algorithmic surveillance of the metadata generated by domestic communications networks to identify security threats.

In the UK and French cases, the CJEU has been called upon to evaluate privacy in intelligence surveillance *internally*, in the activities of *Member State* security and intelligence services. *Schrems II*, which has been decided first, might possibly be a first step in developing a CJEU jurisprudence on privacy in mass surveillance programs. The UK and French cases raise the threshold issue of whether EU fundamental rights law applies in the context of the activities of Member State security agencies. This is tied to the Treaty on European Union's exclusion from EU competences of national security. If the CJEU does find that EU law applies, it will have to address the question of what privacy standards govern in the context of national security surveillance. On this, it is clear from *Schrems II* that independent courts should have oversight and remedial powers but otherwise the judgment is quite vague. The unstable geopolitics and the illiberal developments of the past couple of years highlight the many competing considerations—combating election interference based on the unlawful manipulation of personal data is one of the important activities of national security agencies, yet at the same time expansive surveillance laws threaten rights and, in the case of democratic-backsliding, can be used to consolidate authoritarian rules.
